Attorney Docket No. BHT/3111/127

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BOX PATENT APPLICATION

The Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

Transmitted herewith for filing is a **new utility** patent application of: **Shuning WANN**

Title of Invention: **ENCRYPTION-DECRYPTION DEVICE FOR DATA STORAGE**

Enclosed are:

A specification and 22 claims.

Five (5) sheets of formal drawings (Figs. 1-5).

A Combined Declaration and Power of Attorney

Verified statement to establish **SMALL** Entity Status under 37 CFR § 1.9 and 37 CFR § 1.27.

An Assignment to: **ENOVA TECHNOLOGY CORP.**

The filing fee has been calculated as shown below:

FOR:	NO. FILED	NO. EXTRA	SMALL ENTITY RATE	SMALL ENTITY FEE	LARGE ENTITY RATE	LARGE ENTITY FEE
BASIC FEE				**$355.00**		**$710.00**
TOTAL CLAIMS	**22** -20 =	2	$ 9.	**$18**	$18.	
INDEP CLAIMS	**2** - 3 =	0	$ 40.		$80.	
___ MULTIPLE DEPENDENT CLAIMS			$135.		$270.	
		TOTAL		**$373.00**		$

X A check in the amount of **$413.00** to cover the government filing fee and the Assignment recording fee is enclosed.

X The Commissioner is hereby authorized to charge any additional fees associated with this communication, including patent application filing fees and processing fees under 37 CFR 1.16 and 37 CFR 1.17 or credit any overpayment to **Deposit Account No. 04-1447**. A duplicate copy of this paper is enclosed.

Date: November 3, 2000

Bruce H. Troxell
Registration No. 26,592

DOUGHERTY & TROXELL
5205 LEESBURG PIKE, SUITE 1404
FALLS CHURCH, VIRGINIA 22041
TELEPHONE: (703) 575-2711
FACSIMILE: (703) 575-2707

PTO/SB/10 (1-99)
Approved for use through 9/30/2000. OMB 0651-0031
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

STATEMENT CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f) & 1.27(c))--SMALL BUSINESS CONCERN	Docket Number (Optional)

Applicant, Patentee, or Identifier: **Shuning Wann**
Application or patent No.:
Filed or Issued:
Title: **AN ENCRYPTION-DECRYPTION DEVICE FOR DATA STORAGE**

I hereby state that I am
- ☐ the owner of the small business concern identified below:
- ☐ an official of the small business concern empowered to act on behalf of the concern identified below:

NAME OF SMALL BUSINESS CONCERN **ENOVA TECHNOLOGY CORP.**

ADDRESS OF SMALL BUSINESS CONCERN 10F, No.70, Min-Chuan W. Rd., Taipei, Taiwan, R.O.C.

I hereby state that the above identified small business concern qualifies as a small business concern as defined in 13 CFR Part 121 for purposes of paying reduced fees to the United States Patent and Trademark Office. Questions related to size standards for a small business concern may be directed to: Small Business Administration, Size Standards Staff, 409 Third Street, SW, Washington, DC 20416.

I hereby state that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention described in:
- ☐ the specification filed herewith with title as listed above.
- ☐ the application identified above.
- ☐ the patent identified above.

If the rights held by the above identified small business concern are not exclusive, each individual, concern, or organization having rights in the invention must file separate statements as to their status as small entities, and no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d), or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern, or organization having any rights in the invention is listed below:
- ☐ no such person, concern, or organization exists.
- ☐ each such person, concern, or organization is listed below.

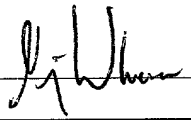
Separate statements are required from each named person, concern or organization having rights to the invention stating their status as small entities. (37 CFR 1.27)

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.38(b))

NAME OF PERSON SIGNING **Shuning Wann**

TITLE OF PERSON IF OTHER THAN OWNER **President**

ADDRESS OF PERSON SIGNING 10F, No.70, Min-Chuan W. Rd., Taipei, Taiwan, R.O.C.

SIGNATURE  DATE November 2, 2000

An encryption-decryption device for date storage

1. Field of the Invention

The present invention relates to an encryption-decryption device for data storage and in particular relates to a data encryption-decryption device provided on the data path connecting a data-generating device and a data storage device to accomplish the purpose of encryption-decryption.

2. Background of the Invention

In the present day of Internet Communications and Electronic Commerce, most businesses and personal matters are carried out on public communication routes. When important or secret information is transmitted and received on these routes, or stored in media without encryption, the risks of unauthorized data access and interception exist. When secrecy and security cannot be assured, the needs for data encryption arise. Data encryption provides a mechanism for protecting data from being unlawfully obtained on storage media or communication routes. In other words, encryption is the process of converting original data to data of incomprehensible form. Being the reverse process of encryption, decryption involves the operation of transforming the encrypted data back to its original fashion. In actual application, data is converted to incomprehensible form before being transmitted on communication routes (e.g., Internet or Local Area Network) or kept in storage media. After completing the decryption process on encrypted data, authorized users obtain usable data in its original form.

A schematic of the prior art encryption is shown in FIG. 1. Data storage and access are executed between a Hard Disk and a Central Processing Unit (CPU). Without processing power of the CPU 2, Encryption Software 3 alone cannot perform the encryption process. As a result, CPU 2

compromises its performance by allocating operational resources per instructions of the Encryption Software 3. To improve the performance of the CPU 2, conventional remedy normally involves adding an acceleration chip 4 between CPU 2 and Encryption Software 3. Since the acceleration chip 4 is not part of the CPU 2, it would require additional cost of purchasing and mounting the acceleration chip 4 on circuit board to raise the performance of the CPU 2. In addition, the necessity for loading Encryption Software 3 on CPU 2 decreases capability thereof, slow down or incapacitate CPU 2 from executing encryption and, consequently, causes inconvenience of using Encryption Software 3, especially when expendable resource or operational performance of the CPU 2 is insufficient. It becomes desirable to find solutions to improve the deficiency.

In order to find a solution, the inventor, after employing a great deal of time and efforts in research, has come up with the present invention for resolving the efficiency problem associated with employing Figure 1's prior art configuration for encryption.

Summary of the Invention

An object of the present invention is to provide a data encryption-decryption device (an IC chip, for instance) for data encryption-decryption such that great improvement is attained when host system resources are relieved of the encryption-decryption process.

Another object of the present invention is to provide a hardware device for allowing direct flow of data and command, on the data path connecting the host and the storage device, such that the existence of the data encryption-decryption device is unknown to either the host or the data storage device. Since the host, the data encryption-decryption device and the storage device are substantially connected serially. From the host's viewpoint, the data encryption-decryption device is regarded as the data storage device. Conversely, from the data storage device's viewpoint, the data encryption-decryption device is regarded as the host. Thus, as far as data

interface and communication is concerned, the data encryption-decryption device is invisible. Therefore, compatibility problems do not exist.

The third object of the present invention is to provide a device capable of making intelligent decisions for distinguishing the types of data received. One example is, if Command or Control signals are detected, the device understands that encryption or decryption would not be required. Whereas, when Data signals are received, the device knows as well that encryption or decryption is to be executed. The devices' decision capability relieves the host from making above decisions, thereby elevating the operational efficiency.

Another preferred embodiment is to place, between the Main Control and the Signal Transmission Line, an Interceptive Device for intercepting data to be encrypted or decrypted according to the Main Control instructions.

Yet another preferred embodiment is to introduce two Data Buffers, one of which is provided between the data encryption-decryption device and the data storage device, and the other buffer provided between the data encryption-decryption device and the data-generating device, for storing pre-decrypted and encrypted data and pre-encrypted and decrypted data, respectively.

The following Description and Designation of Drawings are provided in order to help understand the features and content of the present invention.

Brief Description of the Drawings

The accompanying drawings form a material part of this description, in which:

FIG. 1 is a schematic block diagram of prior art encryption in accordance with the present invention.

FIG. 2 is a schematic block diagram showing the relationship between

Data-generating Device, Data Encryption-Decryption Device and Data Storage Device in the first embodiment of the present invention.

FIG. 3 is a schematic block diagram showing the relationship between Data-generating Device, Data Encryption-Decryption Device and Data Storage Device in the second embodiment of the present invention.

FIG. 4 is a schematic block diagram showing the relationship between Data-generating Device, Data Encryption-Decryption Device and Data Storage Device in the third embodiment of the present invention.

FIG. 5 is a schematic block diagram showing a preferred embodiment of the construction of the Data Encryption-Decryption Device in accordance with the present invention.

Detailed Description of the Preferred Embodiment

The present invention relates to an encryption-decryption device for data storage and in particular relates to a data encryption-decryption hardware device provided serially on the data path connecting a data-generating device and a data storage device for accomplishing encryption-decryption process. The Encryption-Decryption Device provides a novel encryption-decryption construction for improved data encryption (and decryption) and universal system adaptation without comprising the overall system performance.

As shown in Figure 2, the first embodiment of the present invention is a data encryption-decryption device located on the data path. Being an encryption-decryption device serially provided on the data path connecting a data storage device 11 and a data-generating device 13, the data encryption-decryption device 12 serves as a bridge connecting the data storage device 11 and the data-generating device 13. The data encryption-decryption device 12 is capable of performing the encryption-decryption operations independently without utilizing resources of the data-generating device 13, such as CPU, DRAM or other system

resources. From the viewpoint of the data storage device 11, the data encryption-decryption device 12 is regarded as a virtual data-generating device 13. Similarly, from the viewpoint the data-generating device 13, the data encryption-decryption device 12 is treated as a virtual data storage device 11. As far as data interface and communication is concerned, the data encryption-decryption device is invisible. Therefore, data communication between these two devices will function without hindrance.

The above-mentioned data storage device 11 could be any data storage medium, including such storage medium as Hard Disk, Floppy Disk, CD, Magnetic Tape, CD-RW, MO (Magnetic Optical Drive), Digital Video Recorder, Flash Memory Card (FC), PCMCIA Card, and etc.. The data-generating device 13 could refer to any data-generating device, including all data-generating, data-processing and data supplying media as Host Computer, Notebook, Microprocessor, Router and Interface Card, etc. Aided by a software program for encryption-decryption control, the data encryption-decryption device 12 performs the encryption-decryption operation independently. This configuration provides excellent results without compromising overall system performance.

As shown in Figure 3, the second embodiment of the present invention is a data encryption-decryption device being placed on the data path. In this embodiment, a data encryption-decryption device 22 in IC chip form is installed serially on the front end of the designated outgoing transmission interface inside a data storage device 21 (e.g. Hard Disk, Floppy Disk, Flash Memory Card, Digital Video Recorder or CD-RW, etc) such that the control hardware and drivers or the data storage device 21 require no design change. In the form of Socket, IDE, PCI, 1394, SCSI, PCMCIA or USB, etc., the designated outgoing transmission interface allows encryption and decryption of data transmitted between the data storage device 21 and the data-generating device 23. As shown in Figure 4, the third embodiment of the present invention is a data encryption-decryption device being placed on the data path. In this embodiment, a data encryption-decryption device 32, in IC chip form as well, is installed serially on the front end of the designated

outgoing transmission interface, inside a data-generating device 33 (e.g. Host, Notebook, Microprocessor, Flash Memory Card and Interface Card, etc.). In the socket form of IDE, PCI, 1394, SCSI, PCMCIA or USB, etc., the designated outgoing transmission interface allows encryption and decryption of data transmitted between the data storage device 31and the data-generating device 33.

The embodiments in Figures 2 through 4 demonstrate that many varieties of combination can be adopted by the present invention. The data encryption-decryption device, in one example, may be a stand-alone hardware device such as a hub, provided between a data-generating device and a data storage device. It may be, in other examples, installed inside a data-generating device or a data storage device. And can be compatible to IDE, PCI, 1394, SCSI, USB, or other communication interface, it may also act as a designated interface adapting various communication protocols. Therefore, the scope of application for the present invention ranges from the basic data encryption between a single host and its peripheral storage media to those involving connection and communication on the Local Area Networks (LANs) and the Internet.

Figure 5 shows a detailed construction of the Data Encryption-Decryption Device in a preferred embodiment of the present invention, where a data encryption-decryption device is placed on the data path connecting a data-generating device 41 and a data storage device 42, an interceptor 431 is provided such that its one end is connected with said data path and its other end is connected to the main control 432, said main control 432 is electrically connected to a data-generating control device 433, a data storage control device 434 and a data encryption-decryption engine 436, said data encryption-decryption engine 436 is so arranged that its one end is serially connected to an input buffer 435 which in turn is connected to a data-generating device 41, and its other end is serially connected to an output buffer 437 which in turn is connected to a data storage device 42. In addition, the data-generating control device 433 is electrically connected to the data-generating device 41 and the data storage control device 434 is

electrically connected to the data storage device 42.

Based on the above configuration, said main control 432 determines whether incoming data, generated in the data-generating device 41 and subsequently intercepted by the interceptor 431, is to be encrypted (or decrypted) or allowed to pass. Accordingly, the Command or Control Signals are allowed to pass and transmit to the data storage device without encryption. When the data-generating control device 433, the data storage control device 434 and the data encryption-decryption engine 436 are notified of the incoming data, the data-generating control device 433 transmits or receives a Control Signal and act as an interface between the data encryption-decryption device and the data-generating device 41. In other words, communication mode is determined by the interface of the data-generating device 41. For instance, if the data-generating device 41 is a Host and is using IDE interface for communication, IDE protocol will be the communication mode. On the other hand, if the host is equipped with and is using the PCI interface, PCI protocol will become the communication mode. Similarly, as the data storage control device 434 transmits or receives a Control Signal and act as an interface between the data encryption-decryption device and the data storage device 42, various communication modes are involved when designated data is being encrypted or decrypted in response to Control Signals of the main control 44. An input buffer 435 and an output buffer 437 are provided between the data encryption-decryption engine 436 and the data-generating device 41 and between the data encryption-decryption engine 436 and the data storage device 42, for storing pre-encrypted or decrypted data and pre-decrypted or encrypted data, respectively. Said data buffers are also capable of converting the data length. The data-generating device 41 usually has a 1-bit, 8-bit, 16-bit, 32-bit, or 64-bit interface, The input buffer 435 converts incoming data from the data-generating device 41 for encryption and, after encryption, the output buffer 437 then transforms the encrypted data for storage in the data storage device 42.

To recap, the present invention discloses a data encryption-decryption

device serially provided on the data path connecting a data-generating device and a data storage device for encryption-decryption purpose. Since resources of the data-generating device is not involved in the operation, the data encryption-decryption device is capable of accomplishing data encryption-decryption without comprising the overall system performance. By providing corresponding interface capabilities to accommodate both the data-generating device and data storage device, the data encryption-decryption device is transparent to the data-generating devices and data storage devices. Additionally, by adopting suitable data transmission protocols and interface, between the data-generating devices, data encryption-decryption device and data storage devices, as designated interface, the present invention allows the scope of application to extend from encryption between the host and the peripheral storage media to those involving connection and communication on the LANs and the Internet. It is apparent that the present invention discloses novel configurations and provides inventive steps over the prior arts.

While the invention has been described in terms of several preferred embodiments, various alternatives and modifications can be devised by those skilled in the art without departing from the invention. Accordingly, the present invention is intended to embrace all such alternatives that fall within the scope of the claims.

What is claimed is:

1. An encryption-decryption device capable of encrypting and decrypting incoming data, comprising:

a data-generating control device capable of communicating with an external data-generating device;

a data storage control device capable of communicating with an external data storage device;

a data encryption-decryption device for providing encrypting and decrypting functions; and

a control device respectively connecting with the data-generating control device, the data storage control device and the data encryption-decryption device for controlling the same, said control device being capable to determine whether said incoming data need to be encrypted or decrypted by said data encryption-decryption device.

2. The device of claim 1, wherein the data-generating device is a host computer.

3. The device of claim 1, wherein the data-generating device is a notebook computer.

4. The device of claim 1, wherein the data-generating device is a microprocessor.

5. The device of claim 1, wherein the data-generating device is an interface card.

6. The device of claim 1, wherein the data-generating device is a router.

7. The device of claim 1, wherein the data storage device is a hard disk.

8. The device of claim 1, wherein the data storage device is a floppy disk.

9. The device of claim 1, wherein the data storage device is a CD.

10. The device of claim 1, wherein the data storage device is a Magnetic Optical Drive.

11. The device of claim 1, wherein the data storage device is a Digital Video

Recorder.

12. The device of claim 1, wherein the data storage device is a Flash Memory Card.

13. The device of claim 1, further comprising an interceptive device connecting with the main control, said interceptive device being capable of intercepting incoming data for determining if said incoming data need to be encrypted or decrypted by said data encryption-decryption device.

14. The device of claim 1, further comprising a data buffer connected between the data encryption-decryption device and the data-generating device.

15. An encryption-decryption device connecting with a data storage device and a data-generating device via predetermined interfaces, wherein said data encryption-decryption device is a hardware device serially connected between the data storage device and the data-generating device for acting as a bridge for data transmitting there between, said data encryption-decryption device further including a control device and a data encryption-decryption device for encrypting and decrypting at least part of the data.

16. The device of claim 15, wherein said data-generating device is a device choosing from a group consisting of host computer, notebook computer, microprocessor, interface card, and router.

17. The device of claim 15, wherein said data storage device is a device choosing from a group consisting of hard disk, floppy, CD, Flash Memory Card, MO, Digital Video Recorder and PCMCIA.

18. The device of claim 15, wherein said data encryption-decryption device is an IC chip provided within the data-generating device.

19. The device of claim 16, wherein said data encryption-decryption device is serially provided on a front end of the interface located in the data-generating device.

20. The device of claim 15, wherein said data encryption-decryption device is an IC chip provided within the data storage device.

21. The device of claim 20, wherein said data encryption-decryption device

is serially provided on a front end of the interface located in the data storage device.

22. The device of claim 15, wherein said interface is choosing from a group consisting of IDE, PCI, 1394, SCSI, PCMCIA, and USB.

An encryption-decryption device for data storage

Abstract

By incorporating a data encryption-decryption device on the data path connecting a data-generating device and a data storage device, an encryption-decryption device for data storage is disclosed. Input instruction coming from the data-generating device determines whether encryption (or decryption) is to be carried out. If encryption (or decryption) is not called for, data is forwarded directly to a storage device and no encryption process (or decryption process) will be performed. When encryption (or decryption) is required, encryption process (or decryption process) will be executed on the data encryption-decryption engine provided within the data encryption-decryption device. The encryption-decryption device provides a novel encryption-decryption construction for improved data encryption (and decryption) without compromising the overall system performance.

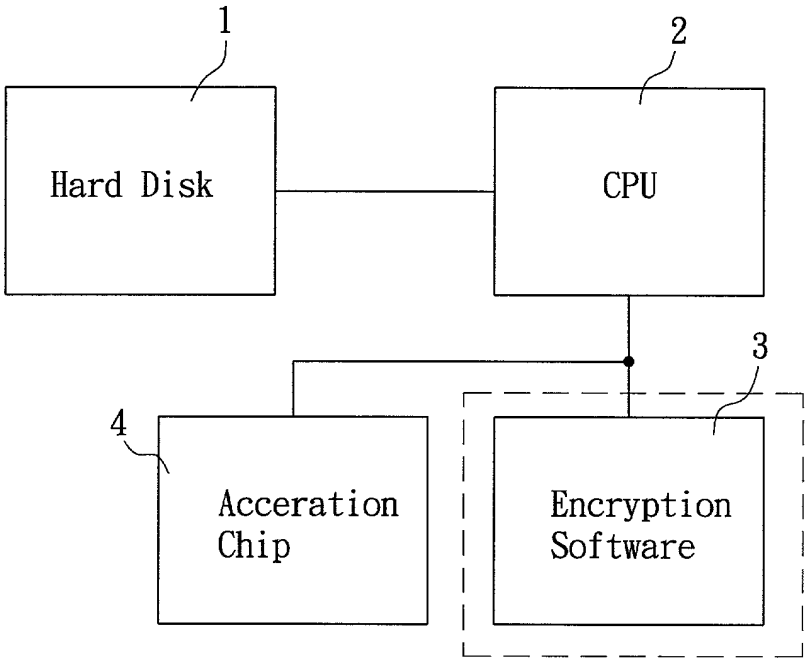


FIG. 1
(PRIOR ART)

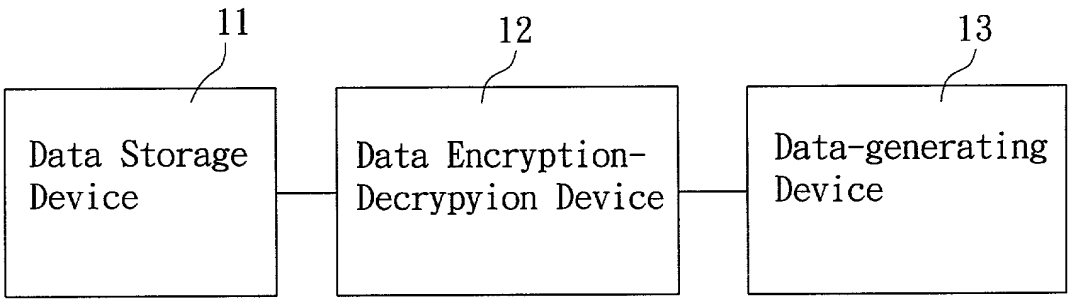

11
12
13
Data Storage Device
Data Encryption-Decrypyion Device
Data-generating Device

FIG. 2

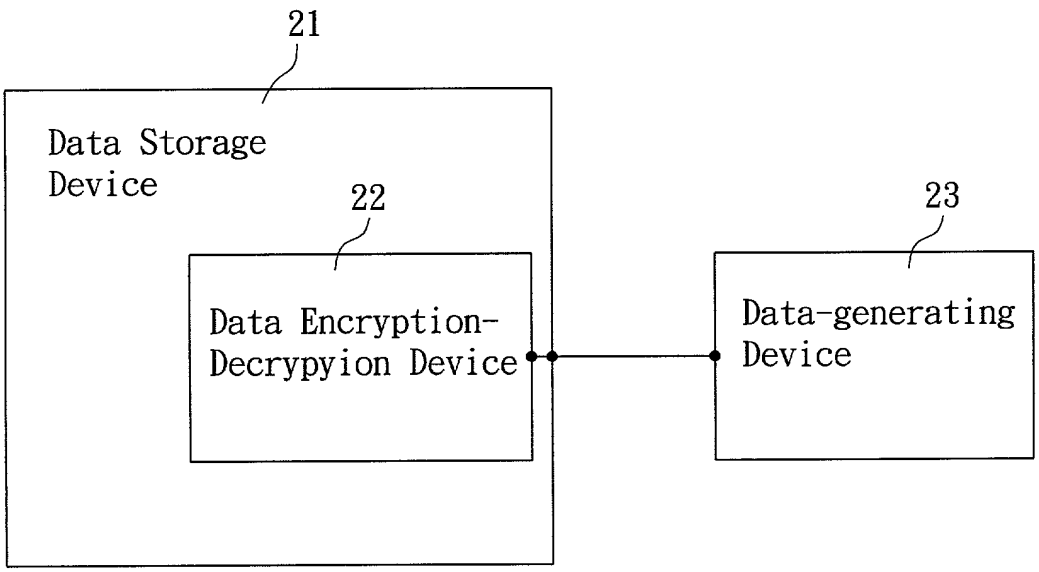

21
Data Storage
Device
22
Data Encryption-
Decrypyion Device
23
Data-generating
Device

FIG. 3

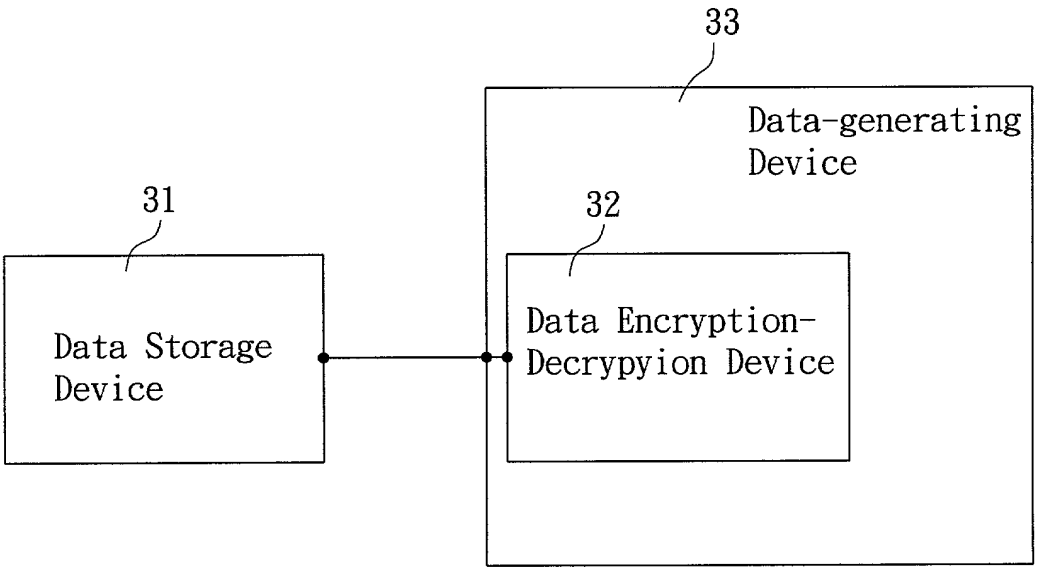

33
Data-generating
Device
31
32
Data Storage
Device
Data Encryption-
Decrypyion Device

FIG. 4

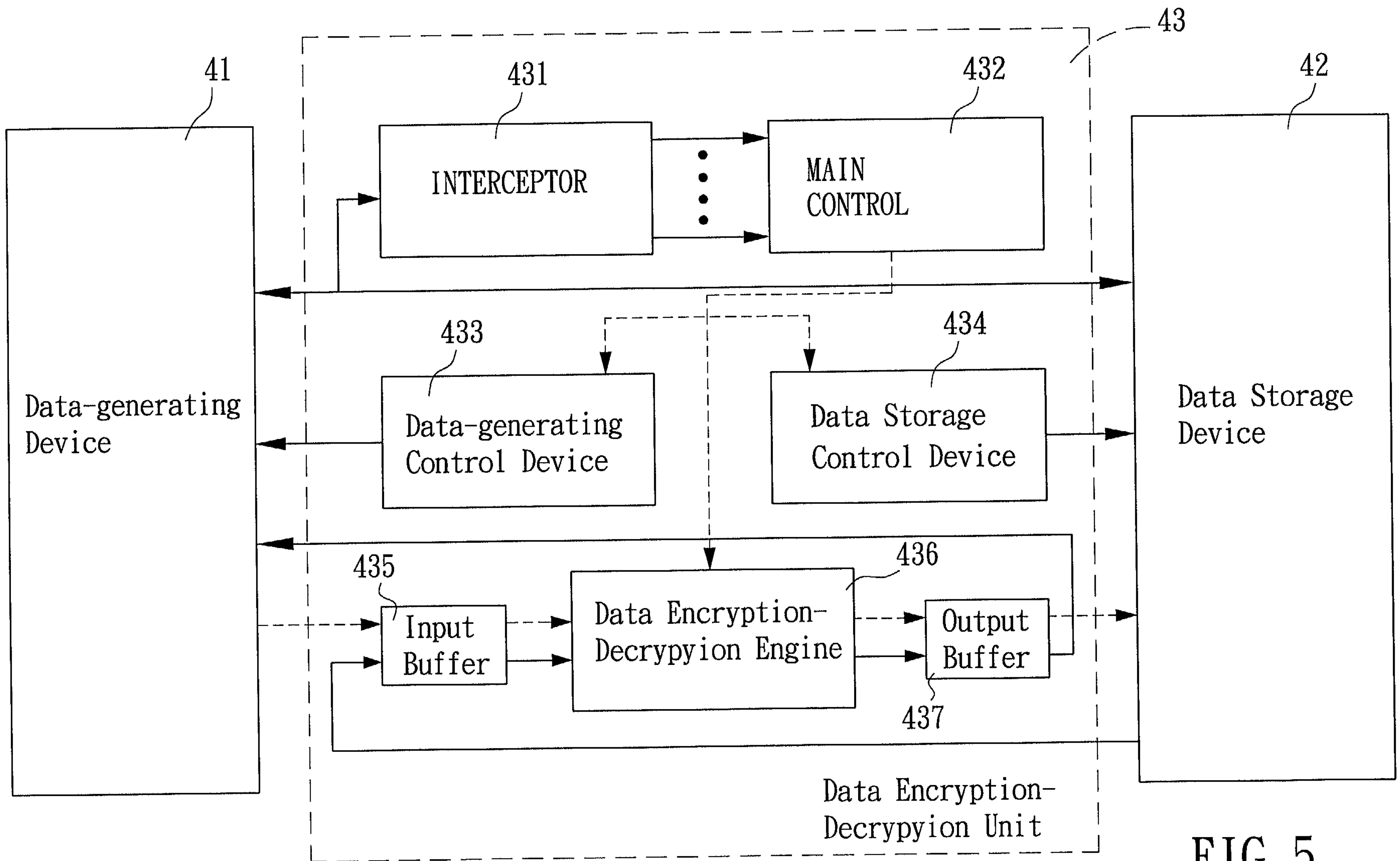

43
41
431
432
42
INTERCEPTOR
MAIN
CONTROL
433
434
Data-generating
Device
Data-generating
Control Device
Data Storage
Control Device
Data Storage
Device
435
436
Input
Buffer
Data Encryption-
Decrypyion Engine
Output
Buffer
437
Data Encryption-
Decrypyion Unit

FIG. 5

ATTORNEY/DOCKET No·

DECLARATION FOR PATENT APPLICATION AND APPOINTMENT OF ATTORNEY

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name; I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention (Design, if applicable) entitled:

AN ENCRYPTION-DECRYPTION DEVICE FOR DATE STORAGE

the specification of which (check one):

□ is attached hereto, or □ was filed on: as U.S. Application Number or PCT International Application Number:
and (if applicable) was amended on:

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment(s) referred to above. I acknowledge the duty to disclose information which is material to patentability as defined in *Title 37, Code of Federal Regulations, .56.* I hereby claim foreign priority benefits under *Title 35, United States Code 19* of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed.

PRIOR FOREIGN APPLICATION(S)			PRIORITY CLAIMED	
Number	Country	Day/Month/Year Filed	Yes	No

□ Additional Priority Application(s) Listed on Following Page(s)

I HEREBY CLAIM THE BENEFIT UNDER TITLE 35 U.S. CODE 119(E) OF ANY U.S. PROVISIONAL APPLICATIONS LISTED BELOW	
Application Number	Day/Month/Year Filed

□ Additional Provisional Application(s) Listed on Following Page(s)

I hereby claim the benefit under *Title 35, United States Code, 20* of any United States application(s) or PCT international application(s) designating The United States of America listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of *Title 35, United States Code, 12,* 1 acknowledge the duty to disclose information which is material to patentability as defined in *Title 37, Code of Federal Regulations, 56* which became available between the filing date of the prior applications) and the national or PCT international filing date of this application:

Application Number	Filing Date	Status - Patented, Pending or Abandoned

□ Additional US/PCT Priority Application(s) listed on Following Page(s)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by line or imprisonment, or both, under *Section 1001 of Title 18 of the United States Code* and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: I (We) hereby appoint as my (our) attorneys, with full powers of substitution and revocation, to prosecute this application and transact all business in the Patent and Trademark Office connected therewith:

David E. Dougherty, Reg. No. 19,576; Bruce H. Troxell. Reg. No. 26,592

I (we) authorize my (our) attorneys to accept and follow instructions from _____ regarding any matter related to the preparation, examination, grant and maintenance of this application, any continuation, continuation-in-part or divisional based thereon, and any patent resulting therefrom, until I (we) or my (our) assigns withdraw this authorization in writing.

SEND CORRESPONDENCE TO: DOUGHERTY & TROXELL
5205 LEESBURG PIKE, SUITE 1404
FALLS CHURCH, VA. 22041

TELEPHONE CALLS TO:
BRUCE H. TROXELL
(703) 575-2711

FULL NAME OF FIRST OR SOLE INVENTOR **Shuning Wann**	CITIZENSHIP Taiwan, R.O.C.
RESIDENCE ADDRESS 10F, NO.70, Min-Chuan W. Rd., Taipei, Taiwan,R.O.C.	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE November 2, 2000	SIGNATURE